UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

United States of America,

Plaintiff,

v.

Terry Lee Carlson, Sr.,

Defendant.

Criminal No. 16-317 (JRT/FLN)

REPORT AND RECOMMENDATION

Carol Kayser for Plaintiff.
Lee Johnson for Defendant Terry Lee Carlson, Sr.

THIS MATTER came before the undersigned United States Magistrate Judge on February 8, 2017, on Terry Lee Carlson Sr.'s motions to suppress statements (ECF No. 22), and to suppress evidence obtained as a result of search and seizure (ECF No. 23). This matter was referred to the undersigned for Report and Recommendation pursuant to 28 U.S.C. § 636 and Local Rule 72.1. At the hearing, the Government offered testimony and entered exhibits into evidence.[1] For the reasons that follow, the Court recommends that Carlson's motions to suppress statements (ECF No. 22) be **GRANTED in part** and **DENIED in part**, and to suppress evidence obtained as a result of search and seizure (ECF No. 23) be **GRANTED**.

I. THE INDICTMENT

On November 16, 2016, a Grand Jury returned the Indictment against Carlson, charging him with five counts of production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and 2251(e); four counts of distribution of child pornography, in violation of 18 U.S.C. §§

1 *See* Exhibit and Witness List, ECF No. 30.

2252(a)(2) and 2252(b)(1); one count of receipt of child pornography, in violation of 18 U.S.C §§ 2252(a)(2) and 2252(b)(1); and one count of possession of child pornography, in violation of U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2). *See* Indictment, ECF No. 1. The Indictment alleges that in 2007 and 2008, Carlson produced five amateur, pornographic videos on an Olympus FE10 camera and Western Digital hard drive, depicting minor children engaged in sexual acts. *Id.* at 1–4. Carlson allegedly distributed this pornographic material via computer file sharing. *Id.* at 4–6. The Indictment also alleges that in 2008, Carlson received a computer file depicting child pornography, and in 2015, knowingly possessed three computer files depicting child pornography. *Id.* at 7–8.

II. FACTUAL BACKGROUND

A. The "Dark Web" and The Tor Network

This case involves a vast and highly publicized investigation of child pornography on what some call, the "dark web."[2] The "dark web," as described by researcher and University of California at Hastings Law School Professor Ahmed Ghappour, is a:

> private global network of computers that enables users to conduct anonymous transactions without revealing any trace of their location. One such private network . . . is the Tor Network. Computers on [the] Tor Network use an encrypted communications protocol that cannot be accessed using normal web browsers; instead, they require the use of special software,

---

2 The investigation of this case has received substantial media coverage. *See, e.g.*, Orin Kerr, *Government 'Hacking' and the Playpen Search Warrant*, Wash. Post, Sept. 27, 2016; Ellen Nakashima, *This is How the Government is Catching People Who Use Child Porn Sites*, Wash. Post, Jan. 21, 2016; Joseph Cox, *The FBI Hacked Over 8,000 Computers in 120 Countries Based on One Warrant*, Motherboard, Nov. 22, 2016, https://motherboard.vice.com/en_us/article/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant; Elizabeth E. Joh, *The Government Shouldn't Distribute Child Pornography*, Jan. 17, 2016, N.Y. Times; Brad Heath, *FBI Ran Website Sharing thousands of Child Porn Images*, USA Today, Jan. 21, 2016, http://www.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn-images/79108346/.

> like the Tor Browser. Proper use of the Tor Network makes it practically impossible for governments to trace the location of computers hosting "hidden" websites on the network, the location of computers accessing those hidden websites, or the location of computers that tunnel through the network to "anonymously" visit public websites on the [standard] World Wide Web.
>
> The Tor Network protects its users from two types of surveillance. First, it protects users from a common form of surveillance called "traffic analysis," which is the real time interception and examination of communications in order to deduce information. Second, it prevents governments from using communications "metadata"—information about a communication, such as its source, destination and size—acquired from third party service providers, to draw conclusions about the communication's parties and their behavior. As a technical matter, use of the Tor Network protects its users' communications from government surveillance because it disassociates communications "metadata" from communications "content" and bounces message packets off several intermediate computers, or "proxies," before steering them to their originally intended destination. Proxy computers are scattered around the globe, provided by people who have volunteered their computers to the anonymity [of the Tor N]etwork. . . .
>
> Thus, someone located in Seattle who has anonymized his or her communications using a series of proxies, the last of which is located in Italy, will, to the destination webpage (e.g., www.google.com or www.facebook. com), appear to be a user in Italy [the exit node]. Likewise, someone in Iran who has run his or her communications through a series of proxies, the last of which is located in San Francisco, will appear to the destination website as a web surfer from San Francisco, and to the local Internet Service Provider ["ISP"] in Iran as though they were attempting to communicate with a proxy computer.[3]

Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. XXX (2017) (in progress).

---

3 The Tor network was originally developed as a project of the United States Naval Research Laboratory for the purpose of encrypting Government communications, but is now available to the public.

Because the Tor network routes communications through a network of assorted computers and exit nodes, the Government claims traditional Internet Protocol ("IP") identification techniques are generally not viable. To investigate illegal activity on the Tor network, law enforcement has developed various network investigative techniques ("NIT") that surreptitiously access target computers remotely. *See* Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 Loy. L. Rev. 315, 316 (2015).

B. The Playpen Website

The Federal Bureau of Investigation ("FBI") began investigating a child-pornographic website known as the Playpen, which had been in operation since April of that year. The Government contends that the Playpen existed as a hidden Tor network service that could only be accessed by connecting to the Tor network and obtaining the specialized Playpen, Uniform Resource Locator ("URL"), from another user from within the Tor network.

In December 2014, a foreign government advised the FBI that it had obtained the IP address of the Playpen, which was being operated from a server owned by the Centrilogic Company ("Centriologic") in Lenoir, North Carolina. On December 23, 2014, the FBI connected to the Playpen website through the Tor network and discovered that it hosted an active message board allegedly dedicated to advertising and distributing child pornography, and contained numerous links to uploaded child pornographic content. The website appeared to have approximately 150,000 users.

In January 2015, the same foreign law enforcement agency advised the FBI that the Playpen IP address had changed, but was still being operated from the Centrilogic server. On January 15, 2015, FBI Special Agent Daniel Alfin applied for a warrant to search the Centrilogic server, and seize, among other things, the Playpen URL and any information that may identify

the Playpen administrator. After that warrant was executed on January 29, 2015, and through further investigation, the FBI determined that the suspected Playpen administrator resided in Naples, Florida. On February 19, 2015, the FBI executed another warrant at the Naples residence. The FBI apprehended Steven W. Chase, the alleged Playpen administrator, and assumed control of the website.[4] Rather than shut the website down, the FBI continued to operate an identical copy of the Playpen, including distribution of the alleged child pornography housed on the website, through a Government controlled server, located in Newington, Virginia.

C. The NIT Warrant

The FBI then obtained a Title III warrant pursuant to 18 U.S.C. § 2518, to monitor and intercept user communications on the Playpen website. Given the anonymizing capabilities of the Tor network, the FBI claims that it was unable to identify the website's users using traditional investigative techniques. On February 20, 2015, FBI Special Agent Douglas Macfarlane filed a warrant application to use what the Government calls an NIT to assist the FBI in identifying Playpen's users and other potential website administrators. The warrant application was presented to a United States Magistrate Judge for the Eastern District of Virginia.

In his affidavit in support of the warrant application, Special Agent McFarlane represented that the NIT would be deployed on the computer of any Playpen user entering the website through an individualized login name and password, regardless of the user's physical location. The NIT functions as a form of malware, implanting itself on a Playpen user's computer and forcing the computer to "activate," or to transmit identifying packets of information back to the Government controlled server in Virginia. When the search warrant was

---

4 Chase was later convicted of engaging in a child exploitation enterprise and running a website dedicated to the sexual abuse of children. *See* Department of Justice Office of Public Affairs Announcement, https://www.justice.gov/opa/pr/florida-man-convicted-engaging-child-exploitation-enterprise, Sept. 16, 2016.

issued, neither the Government nor the issuing Magistrate Judge had any idea which computers, out of all of the computers on the planet, might be infected by the Government's invasive malware. The identifying packets of data that the NIT extracts from a user's activating computer include: the IP address; the date and time the NIT ascertained the IP address; a unique identifier generated by the NIT to distinguish data from different activating computers; the type of operating system running on the activating computer, including type, version, and architecture; information on whether the NIT had already been delivered to the activating computer; the host name of the activating computer; the operating system used by the activating computer; and the Media Access Control address of the activating computer.

The Magistrate Judge approved the NIT warrant and authorized the FBI to deploy the NIT malware for thirty days. The Magistrate Judge further granted a request by the FBI to delay notice of the search until thirty days after any individual accessing the Playpen website had been identified to a sufficient degree as to provide the required notice pursuant to 18 U.S.C. § 3103(a)(b) and Federal Rule of Criminal Procedure 41(f)(3).

The FBI deployed the NIT malware from February 20, 2015, through March 4, 2015, at which time it took the Playpen website offline. During that time, the Government itself operated the website and facilitated the global distribution of content containing depictions of child pornography. Although the Court is not aware of the precise number, testimony in other cases has established that during the period in which the FBI ran the illegal website, the NIT targeted tens of thousands of activating computers located in over 120 countries through the use of a satellite provider. *See, e.g.*, *United States v. Michaud*, 15-cr-5351, 2016 WL 337263, (W.D. Wash. Jan. 28, 2016) ECF No. 126 at 18–19 ("I may say if this was only this defendant and the argument was outrageous government, conduct, it would be a much different argument than if

this was 10,000 people, in terms of where it was outrageous or not. I mean it's one thing to go after one person that you think is committing a crime, and something different to go after everybody under the sun on the same premise") (quoting District Judge Robert J. Bryan); (*United States v. Tippens*, 16-cr-5110, ECF No. 103 at 17–18. (W.D. Wash. Nov. 1, 2016) ("[t]here's just another layer of fact there that we did not know about. I mean, we did not know this was a truly global warrant before. There are 120 countries and territories listed outside the United States that the FBI hacked into, and they also hacked into something called a 'satellite provider.' So now we are into outer space as well.").

Stated differently, the Government claims legal authority from this single warrant, issued in the Eastern District of Virginia, to hack thousands of computers in 120 countries and to install malicious software for the purpose of investigating and searching the private property of uncounted individuals whose identities and crimes were unknown to the Government before launching this massive worldwide search. *See e.g.*, *United States v. Kahler*, 16-cr-2055, 2017 WL 586707 *1 (E.D. MI Feb. 14, 2017) (stating that "on February 20, 2015, a federal magistrate judge in the Eastern District of Virginia signed a warrant authorizing a FBI hacking operation designed to infiltrate a suspected child pornography website, named 'Playpen.'").

D. Search and Statements

According to data obtained from the NIT deployment, a user named "waytocool" accessed the Playpen website for a total of 25.06 hours between December 2014, and March 2015. On February 23, 2015, "waytocool" entered the website and allegedly downloaded content on a post entitled "SOBRENAS," in the pre-teen section of the website. Through the NIT, the FBI was able to determine that user "waytocool" was connected to a server operating at IP address 173.23.28.89, and the activating computer named "Terryr-PC." Through public sources,

the FBI determined that the IP address was operated by Mediacom Communications Corporation ("MCC"). On March 1, 2015, and March 4, 2015, "waytocool" again entered the Playpen website and allegedly downloaded multiple images that depict child pornography.

In mid-March 2015, an administrative subpoena was served on MCC requesting information related to the assigned user of IP address 173.23.28.89. MCC reported that the IP address was assigned to a private residence in Waseca, Minnesota. On July 10, 2015, FBI Special Agent Glenn Moule obtained postal records showing that Carlson is the only person who received mail at the Waseca, Minnesota address.

On October 22, 2015, Agent Moule presented a search warrant application to a Magistrate Judge in the District of Minnesota. The warrant requested authorization to search Carlson's residence. The affidavit supporting the warrant included much of the same facts as set forth in the affidavit supporting the NIT warrant application. In addition, Carlson's alleged entry and conduct on the Playpen website is described, as is the information seized pursuant to the NIT's deployment on Carlson's activating computer earlier that year.

On November 2, 2015, Agent Moule executed the search warrant at Carlson's Waseca, Minnesota residence. Testimony at the February 8, 2017, hearing, established that Agent Moule and the search team arrived at Carlson's residence at approximately 9:00 a.m. Carlson was not home at that time, but he returned home soon after the search began. Carlson was promptly interviewed by Agent Moule and FBI Special Agent Christopher Blackmore when he returned. Shortly after the interview began, Carlson fainted and Agent Moule summoned an ambulance. Carlson quickly revived, and declined medical treatment once the ambulance arrived. The interview then immediately resumed.

Carlson was not handcuffed during the interview and moved freely about his residence. Approximately one hour into the interview, Carlson requested that the interview move to a local park. That request was granted and Carlson drove himself to the local park, where the interview continued. During the course of the interview, Carlson stated that he was attracted to, and fascinated by, child pornography and that he had struggled with his attraction for many years. In addition, Carlson admitted to entering the Playpen website.

During the search of Carlson's residence, the FBI seized twenty electronic devices. A forensic review of an Antec computer allegedly showed that Carlson had entered the Playpen website and downloaded child pornography. A subsequent review allegedly showed that Carlson had produced child pornography on a Western Digital hard drive.

A year later, on November 17, 2016, Agent Moule executed a second warrant, issued by a different United States Magistrate Judge in the District of Minnesota, for Carlson's residence, now located in Coleraine, Minnesota. At this time, Agent Moule arrested Carlson. Shortly thereafter, Agent Moule and FBI Special Agent Craig Hedidenreich interviewed Carlson in a breakroom at the Coleraine Police Department. Before the interview began, Carlson signed an Advice of Rights form, apprising him of his: right to remain silent; that anything he said could be used against him in court; the right to an attorney and to have an attorney appointed if he could not afford legal assistance; and the right to terminate the interview. During the interview, Carlson made inculpatory statements regarding the production and possession of child pornography.

III. CONCLUSIONS OF LAW

A. Motion to Suppress Evidence (ECF No. 23)

Carlson moves to suppress all evidence seized pursuant to the NIT warrant, as well as derivative evidence, seized pursuant to the subsequent Minnesota warrants as fruits of the poison

tree under *Wong Sun v. United States*, 371 U.S. 471 (1963), and its progeny. Def.'s Mem. in Supp. 6, 19, ECF No. 24. Sequentially, Carlson argues that: (1) the NIT warrant issued in the Eastern District of Virginia violated 28 U.S.C. § 636(a) of the Federal Magistrate Judge Act, Federal Rule of Criminal Procedure 41(b), and the Fourth Amendment particularity requirement, and the search of his computer in Minnesota exceeded the scope of the NIT warrant; (2) as a result of these violations, all evidence obtained pursuant to the NIT warrant must be suppressed; (3) evidence seized pursuant to the 2015 and 2016 Minnesota warrants must also be suppressed because the probable cause supporting their issuance was derived solely from the evidence seized pursuant to the NIT warrant; and (4) the *Leon* good-faith exception does not apply to the facts of this case. *Id.* at 19. The Government contends that the NIT warrant satisfies the Fourth Amendment particularity requirement, was authorized by Rule 41(b), and even assuming a violation occurred in the issuance of the NIT warrant, suppression is not required because of the *Leon* good-faith exception to the exclusionary rule. Opp'n Mem. 8, 13, 22, ECF No. 25.

As a threshold matter, the Government does not challenge Carlson's assertion that the deployment of the NIT malware on his activating computer was a Fourth Amendment search. ECF No. 24 at 7. This Court is aware of no lawful way for the Government to deploy this investigative technique. Assuming without deciding that some lawful way could be devised to use the technology employed here, the Court concludes that the Government, by using the NIT malware to collect data from Carlson's activating computer conducted an unlawful search that was not supported by a lawful warrant. Likewise, the Government's attempted work around of the Fourth Amendment fails to qualify as a recognized warrant exception. *See United States v. Croghan*, No. 1:15-cr-48 (S.D. Iowa Sept. 19, 2016) (reasoning that because the NIT obtained identifying packets of information directly from the defendants' activating computers, a valid

search warrant, or warrant exception was required). For the reasons set forth more fully below, the unlawful search of Carlson's computer is not saved by the good-faith exception to the exclusionary rule.

1. The NIT Warrant Violated the Federal Magistrate Judge Act and Federal Rule of Criminal Procedure 41(b)

Carlson argues that the Magistrate Judge, sitting in the Eastern District of Virginia, exceeded her territorial jurisdiction in authorizing the deployment of the NIT malware and consequent search and seizure of any activating computer located outside of that District *Id.* at 9. The Court agrees.

The Federal Magistrate Judge Act, 28 U.S.C. § 636(a), and Federal Rule of Criminal Procedure 41(b) limit a magistrate judge's territorial authority to issue warrants. 28 U.S.C. § 636(a) provides that a United States "Magistrate Judge . . . shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where the court may function, and elsewhere as authorized by law" certain duties, including among other things "all powers and duties conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts." 28 U.S.C. § 636(a)(1). Rule 41(b) provides, in relevant part:

> **Authority to Issue a Warrant**. At the request of a federal law enforcement officer or an attorney for the Government:
>
> (1) a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> . . .

> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both . . .

Fed. R. Crim. P. 41(b).[5]

Neither Rule 41(b)(1) nor 41(b)(2) authorized the Magistrate Judge, sitting in the Eastern District of Virginia, to issue the so called NIT warrant. Those provisions of Rule 41(b) limit a magistrate judge's authority to issue warrants for the search of property "located within the district" at the time the warrant issues. Here, only the Government controlled server housing the Playpen website was located in the Eastern District of Virginia. Crucially, the identifying packet of information sought through the NIT's deployment was stored on Carlson's activating computer, which at all relevant times was located in Minnesota.

The Government argues that the NIT warrant is a valid tracking-device under Rule 41(b)(4), because the NIT was an electronic tool deployed for the purpose of tracking the movement of information both within and outside the Eastern District of Virginia. ECF No. 25 at 13. However, a Rule 41(b)(4) "tracking device" is defined as any "electronic or mechanical device which permits the tracking of the movement of a person or object." Fed. R. Crim. P. 41(a)(2)(E); 18 U.S.C. § 3117(a)–(b). Here, the NIT malware did not track the movement of a person or object. Instead, the electronic information traveled to Carlson's activating computer in Minnesota, and once implanted, the NIT merely directed that an identifying packet of other electronic information be relayed back to the Government server in Virginia. In addition, even assuming the NIT was a tracking device, the Magistrate Judge in the Eastern District of Virginia still exceeded her territorial jurisdiction because the NIT was installed on Carlson's activating

5 Fed. R. Crim. P. 41 was amended on December 1, 2016.

computer in Minnesota, not in the Eastern District of Virginia. *See* Fed. R. Crim. 41(b)(4) (providing that "a magistrate judge with authority in the district has authority to issue a warrant to install *within the district* a tracking device") (emphasis added).

In addition, the Court notes that the FBI "itself did not believe the NIT was a tracking device." Pl.'s Supp. Mem. 9, ECF No. 34. A tracking-device warrant must comply with procedures outlined in Rule 41(e)(2)(C) and 41(f)(2)(A)–(C). For example, Rule 41(e)(2)(C) requires that "a tracking device warrant must identify the person or property to be tracked, designate the magistrate judge to whom it must returned, and specify a reasonable length of time that the device may be used." Fed. R. Crim. P. 41(e)(2)(C). Here, the return of the NIT warrant does not identify a device being installed or returned to the issuing Magistrate Judge. Similarly, an officer executing "a tracking-device warrant must enter on it the exact date and time the device was installed and the period in which it was used," Fed. R. Crim. P. 41(f)(2)(A), but, there is no mention of an exact date and time in which the NIT was installed on Carlson's activating computer. Given that the NIT warrant does not reference tracking procedures or the installation of tracking devices, the Court declines the Government's invitation to infer that the FBI sought authorization of the NIT warrant under Rule 41(b)(4).

This Court joins the several courts that have concluded that the Magistrate Judge in the Eastern District of Virginia lacked authority to issue the NIT warrant pursuant to Rule 41(b)(4). *See, e.g.*, *United States v. Torres*, No. 5:16-cr-285, 2016 WL 4821223, at *6 (W.D. Tex. Sept. 9, 2016) (holding that it "is inappropriate for this Court to engage in a process of finesse justifying an ethereal presence of the defendant's computer in Virginia, where the plain language of [Rule 41(b)(4)] as now written does not provide jurisdiction under these circumstances"); *United States v. Henderson*, No.15-cr-565, 2016 WL 4549108, at *3 (N.D. Cal. Sept. 1, 2016) (reasoning that

the NIT warrant search fails the requirements of 41(b)(4) because, "even though it was analogous to a tracking device in some ways, it nevertheless falls outside the meaning of a tracking device as contemplated by the rule. Further, the NIT was installed outside of the district, at the location of the activating computers, not within the district as required" by Rule 41(b)(4)); *United States v. Werdene*, No. 15-434, 2016 WL 3002376, at *7 (E.D. Pa. May 18, 2016) (finding Rule 41(b)(4) inapplicable because it is "premised on the person or property being located within the district" and because it is "uncontested that the computer information that the NIT targeted was at all relevant times located beyond the boundaries of the Eastern District of Virginia"); *United States v. Levin*, 186 F. Supp. 3d 26, 28 (D. Mass. May 5, 2016) (rejecting the argument that the transmittal of the NIT to activating computers to "the installation of a tracking device in a container holding contraband"); *United States v. Arterbury*, No. 15-cr-182 (N.D. Okla. Apr. 25, 2016) (concluding that the "NIT warrant was not for the purpose of installing a device that would permit authorities to track the movements of Defendant or his property"); *Michaud*, 2016 WL 337263, at *6 (concluding that "applying the tracking device exception fails, because the defendant's computer was never physically located within the Eastern District of Virginia.").

In sum, the issuance of the NIT warrant violated the Federal Magistrate Judge Act and Federal Rule of Criminal Procedure 41(b).

2. All Evidence Derived From the Use of the NIT Warrant Must be Suppressed

Finding a violation of Rule 41(b), the Court must fashion an appropriate remedy. "Rule 41 and the Fourth Amendment are not coextensive," and "[n]oncompliance with [Rule] 41 prerequisites do not automatically require the exclusion of evidence in a federal prosecution." *United States v. Schoenheit*, 856 F.2d 74, 76–77 (8th Cir. 1988). "Absent a constitutional

infirmity, the exclusionary rule is applied only to violations of Federal Rule 41 that prejudice a defendant or show reckless disregard of proper procedure." *United States v. Hyten*, 5 F.3d 1154, 1157 (8th Cir. 1993) (citing *United States v. Freeman*, 897 F.2d 346, 348–49 (8th Cir. 1990)); *see also United States v. Welch*, 811 F.3d 275, 280–81 (8th Cir. 2016) (stating that a defendant "must show, [that] the Rule 41 violation [1) was of constitutional import]; [or] 2) either that he was prejudiced by the violation or that the investigators recklessly disregarded proper procedure").

a. Constitutional Infirmity

Three Courts have held that the NIT warrant's violation of Rule 41(b) constituted a constitutional infirmity.[6] Specifically, those courts concluded that because the Magistrate Judge in the Eastern District of Virginia lacked territorial jurisdiction to issue the NIT warrant, the warrant was void *ab initio*, or as if the warrant never existed. This Court agrees.

Rule 41, has both procedural and substantive provisions. Courts presented with violations of Rule 41's ministerial or technical procedural provisions have generally determined that suppression of evidence is unwarranted.[7] This case, however, involves a violation of Rule 41(b), the provision of Rule 41 that defines the source and outer limits of a magistrate judge's authority to issue warrants under federal law. *See e.g.*, *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008) (reasoning that Rule 41(b) is a substantive, not procedural, provision, and unlike other provisions of Rule 41, Rule 41(b) is entitled "authority to issue warrants"); *see also United States v. Krueger*, 809 F.3d 1109, 1115 n.7 (10th Cir. 2015) (concluding that Rule 41(b)(1) "is unique from other provisions of Rule 41 because it implicates substantive judicial authority," and

---

6 *See Levin*, 186 F. Supp. 3d at 38; *Arterbury*, 15-cr-182 (N.D. Okla. Apr. 25, 2016); *Croghan*, 15-cr-48 (S.D. Iowa Sept. 19, 2016).

7 *See Levin*, 186 F. Supp. 3d at 35, n.10 (collecting cases).

reasoning that cases involving violations of other subsections of Rule 41 "offer limited guidance") (internal quotation marks and citations omitted). The Rule 41 violation here was not simply technical or ministerial. *See United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013) (concluding that a Rule 41(b) violation constitutes a fundamental jurisdictional flaw that cannot "be excused" as a technical defect); *Croghan*, 15-cr-48 (S.D. Iowa Sept. 19, 2016) (concluding that "because the magistrate judge lacked authority, and thus jurisdiction, to issue the NIT warrant as required by the Fourth Amendment, . . . the NIT warrant was void *ab initio*, akin to no warrant at all.").

"Because the violation here involved 'substantive judicial authority' rather than simply 'the procedures for obtaining and issuing warrants,'" the Court concludes that the Rule 41(b) defect in the NIT warrant was substantive. *Levin*, 186 F. Supp. 3d at 36 (quoting *Krueger*, 809 F.3d at 1115 n.7). Indeed, because the Magistrate Judge in the Eastern District of Virginia lacked authority, and thus jurisdiction, to issue the NIT Warrant, there was no judicial approval of the NIT warrant. *See id.* (collecting cases in which the court held that an authorized signature on the search warrant by the person authorized to issue it is essential to a warrant's fundamental constitutional validity). Accordingly, the NIT warrant is void *ab initio*. Without an identifiable warrant exception (the Government offers none and the Court is aware of none) the Court concludes that the NIT warrant's violation of Rule 41(b) and 28 U.S.C. § 636(a) constitutes a constitutional infirmity. *See Hyten*, 5 F.3d at 1157.

b. Prejudice and Reckless Disregard of Proper Procedure

In the Eighth Circuit, prejudice is found where "the search might not have occurred or would not have been so abrasive if the Rule had been followed," and reckless disregard may be found where "there is evidence of intentional and deliberate disregard of a provision in the

Rule." *Freeman*, 897 F.2d at 346, 349–50 (quoting *United States v. Burke*, 517 F.2d 377, 386–87 (2d Cir. 1975)). Here, neither the search of Carlson's activating computer pursuant to the NIT warrant nor the searches pursuant to the two warrants issued in the District of Minnesota would have occurred without the violation of Rule 41(b). Had Rule 41(b) been complied with, the FBI would not have obtained the identifying information from Carlson's activating computer or Carlson's IP addresses, would not have been able to link that IP addresses to Carlson's residence through subsequent investigation and administrative subpoenas, and would not have had sufficient evidence to support a probable cause showing to obtain the warrants issued in the District of Minnesota. Carlson has satisfied his burden to prove that the several searches at issue would not have occurred if there had been compliance with Rule 41(b). *See Freeman*, 897 F.2d at 350.

The Government, relying on *Welch*, argues that the operative question is not whether the "same judge could have issued the NIT Warrant in compliance with Rule 41(b), but whether the search would have occurred had the rules been followed." ECF No. 25 at 20; *see Welch*, 811 F.3d at 281. The Government argues that Agent Macfarlane could have secured the NIT warrant by presenting it to a district court judge in the same district. *See id.* at 21.[8] The Court is not persuaded. First, *Welch* did not examine prejudice in the context of a magistrate judge's statutory authority to issue warrants under Rule 41(b), but instead under the procedural, notice provisions of Rule 41(f). As such, *Welch* is inapposite. The operative inquiry, rather, is whether the "search might not have occurred . . . if the *Rule* had been followed." *Freeman*, 897 F.2d at 349–50 (emphasis added). Here, neither rule, 41(b) nor § 636(a), permitted the Magistrate Judge in the

8 This Court expresses no opinion on whether, under these circumstances, a district court judge in the Eastern District of Virginia has any more authority than a magistrate judge to issue a warrant to search property in Minnesota. Suffice it to say, no such warrant was issued here.

Eastern District of Virginia to approve the use of the NIT malware to search Carlson's activating computer in Minnesota.

In addition, the Court concludes that in requesting the NIT warrant, Agents recklessly disregarded proper procedure. *Hyten*, 5 F.3d at 115. The Government argues that Agents should not be blamed for the Magistrate Judge's error in issuing a defective warrant, or for, ostensibly, not knowing the ambit of magistrate judge authority. *See* ECF No. 25 at 27. However, the Court will not impute that level of legal ignorance given that Agent Macfarlane, in applying for the NIT warrant, was familiar with the procedure for extending notice under 18 U.S.C. § 2705 and requested use of the NIT malware under Rule 41. Moreover, there was an obvious conflict between the issued warrant, which on its face, was limited to searches in the Eastern District of Virginia, and Agent Macfarlane's affidavit, which sought to search activating computers, wherever on the planet that they were located.

The search warrant application and the warrant, as issued, expressly limit themselves to the search of persons or property located in the Eastern District of Virginia. Yet paragraph forty-six of Agent Macfarlane's affidavit explains in some detail how the NIT malware might be deployed anywhere on earth. Specifically, paragraph forty-six provides that "the NIT may cause an activating computer – wherever located – to send to a computer controlled or known to the government, network level messages containing information that may assist in identifying the computer." Under these circumstances, Agent Macfarlane must have known that he was acting in reckless disregard of proper procedure. It was not objectively reasonable for Agent Macfarlane, a "law enforcement . . . veteran" employed by the FBI "for 19 years" to believe that the NIT warrant, which he knew could reasonably reach any computer in the world, was properly issued given the specific territorial limits under Rule 41(b) and the language of the warrant itself, which

limited searches to the Eastern District of Virginia. *See Levin*, 186 F. Supp. 3d at 43. Put differently, it was not objectively reasonable for Agents to believe that a single warrant, which by its terms was explicitly limited to searches in the Eastern District of Virginia, could be used to electronically search Carlson's computer in Minnesota or any of the other countless computers around the world. That the issuing Magistrate Judge recklessly disregarded the limits of her own authority under Rule 41(b) does nothing to change the fact that the Rule 41(b) violation was accompanied by reckless disregard for proper procedure. Indeed, in light of all of the facts and circumstances surrounding the issuance of the extraordinary NIT warrant, it would not be unreasonable to infer that the disregard of proper procedure was deliberate given the inconsistencies between paragraph forty-six in Agent Macfarlane's affidavit and the cover sheet of the warrant application and the warrant itself.

In short, the Court concludes that the issuance of the NIT warrant in violation of Rule 41(b) was of constitutional magnitude, prejudiced Carlson, and was done in reckless disregard of proper procedure.

c. Leon Good-Faith Does Not Apply

Having determined that the NIT warrant was void, the Court must determine whether suppression of the evidence found during the search of Carlson's activating computer and residence is warranted. "Only a 'fundamental' violation of Rule 41 requires automatic suppression, and a violation is 'fundamental' only where it, in effect, renders the search unconstitutional under traditional [F]ourth [A]mendment standards." *Freeman*, 897 F.2d at 349 (quoting *United States v. Luk*, 859 F.2d 667, 671 (9th Cir. 1988). In *United States v. Leon*, 468 U.S. 897 (1984), and its companion case, M*assachusetts v. Sheppard*, 468 U.S. 981 (1984), the Supreme Court established a good-faith exception to the Fourth Amendment exclusionary rule.

Under the good-faith exception, evidence obtained pursuant to a warrant later determined to be invalid is admissible if the executing officer's reliance on the issued warrant, and belief that the issued warrant was valid, was reasonable. *See Leon*, 468 U.S. at 922; *see also United States v. Clay*, 646 F.3d 1124, 1127 (8th Cir. 2011) ("[T]he exclusionary rule should not be applied so as to bar the admission of evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate, even if that search warrant is later held to be invalid.") (citing *Leon*, 468 U.S. at 900, 922)). The constitutional rationale for the good-faith exception is that there is inadequate deterrent value to justify application of the exclusionary rule when police obtain a warrant, reasonably relying on its validity, only to later learn that the magistrate judge erred in authorizing the search. *See Leon*, 468 U.S. at 921. The Court reasoned in *Leon*, that "[p]enalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Id.*

Whether *Leon* should apply in instances of a void warrant is a matter of first impression in the Eighth Circuit. The Supreme Court has opined that "reasonable minds frequently may differ on the question of whether a particular affidavit establishes probable cause, and we have thus concluded that the preference for warrants is most appropriately effectuated by according great deference to a magistrate judge's determination." *Leon*, 468 U.S. at 914. The Government argues that *Leon* and its progeny do not, "as a categorical matter limit the reach of the good-faith exception." ECF No. 25 at 23.

However, the good-faith exception, as constructed in *Leon*, does not stand for the improvident proposition that great deference should be extended to a magistrate judge deliberately or recklessly exercising authority inimical to the source of her statutory power to issue a warrant. Indeed, the *Leon* good-faith exception is predicated on a finding that a warrant,

in fact, was issued. *See Levin*, 186 F. Supp. 3d at 38 (reasoning that *Leon* "contemplated two circumstances: one in which a warrant is issued and is subsequently found to be unsupported by probable cause and the other in which a warrant is supported by probable cause, but is technically deficient."); *see also Herring v. United States*, 555 U.S. 135, 146 (2009) (explaining that in *Leon*, the Court "held that the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search cannot justify the substantial costs of exclusion. The same is true when evidence is obtained in objectively reasonable reliance on a warrant subsequently recalled.").

Here, the NIT warrant was void *ab initio*, akin to no warrant at all. Therefore, there was no issued, but subsequently invalidated or recalled warrant for officers to objectively rely upon. "To hold that the good-faith exception is applicable here would collapse the distinction between a voidable and a void warrant." *Levin*, 186 F. Supp. 3d at 41. As other courts have reasoned, the distinction is significant, as a voidable warrant "involves judicial error, such as the misjudging the sufficiency of the evidence" or a finding of probable cause. *Id.* Conversely a void warrant, as is the case here, is a substantive, non-technical, defect that implicates the fundamental judicial authority and statutory power conferred upon a magistrate judge to issue warrants in the first instance. *See id.* (collecting cases that have held that the *Leon* good-faith exception presupposes that the disputed warrant was issued by a neutral and detached magistrate judge imbued with the requisite legal authority). The Court notes that the good-faith exception left "untouched the probable-cause standard and the various requirements for a valid warrant." *Leon*, 468 U.S. at 923. To the extent that *Leon* cleaved a good-faith Fourth Amendment exception to the exclusionary rule, that exception cannot apply when the requirements for the very authority and

jurisdiction of the magistrate judge to issue a warrant were abandoned. Therefore, the Court concludes that the *Leon* good-faith exception does not apply in this case.

d. The Searches of Carlson's Residence

The searches of Carlson's residences in November 2015, and in November 2016, were fruits of the defective NIT warrant. The Government does not appear to contest that these searches were derivative of the NIT warrant. Therefore, evidence seized pursuant to the searches of Carlson's residences must be suppressed. *See Wong Sun*, 371 U.S. at 488.

e. Summation

- The NIT Warrant was issued in violation of 28 U.S.C. § 636(a) and Federal Rule of Criminal Procedure 41(b)
- The violation was not ministerial nor technical because it implicated the substantive judicial authority of the issuing Magistrate Judge
- The NIT warrant was void *ab initio*
- That violation was of constitutional magnitude under the Fourth Amendment, prejudiced Carlson, and recklessly disregarded proper procedure
- The *Leon* good-faith exception to the exclusionary rules does not apply when the issued warrant is void *ab initio*
- Suppression of the evidence derived from the NIT warrant is the appropriate remedy on the facts of this case
- Carlson's motion to suppress evidence obtained as a result of search and seizure must be granted

3. The NIT Warrant Lacked Particularity

Independent of the foregoing, this Court concludes that all of the evidence derived from the NIT warrant must be suppressed because the NIT warrant also violated the Fourth Amendment's particularity clause.[9]

The Warrant Clause of the Fourth Amendment prohibits the issuance of a warrant, except one "particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. In the Eighth Circuit, "[t]he particularity requirement 'is a standard of practical accuracy rather than a hypertechnical one." *United States v. Fiorito*, 640 F.3d 338, 346 (8th Cir. 2011) (quoting *United States v. Thurman*, 625 F.3d 1053, 1057 (8th Cir. 2010)). "[W]hether a warrant fails the particularity requirement cannot be decided in a vacuum. The court will base its determination on such factors as the purpose for which the warrant was issued, the nature of the items to which it is directed, and the total circumstances surrounding the case." *Milliman v. Minnesota*, 774 F.2d 247, 250 (8th Cir. 1985) (internal citations omitted); *see also Andresen v. Maryland*, 427 U.S. 463, 480 (1976).

This Court concludes that the NIT warrant lacks particularity because it is not possible to identify with any specificity, which computers, out of all of the computers on earth, might be searched pursuant to this warrant. Put differently, the NIT warrant fails to particularly describe the place to be searched. Attachment A to the NIT warrant purports to be the description of the "place to be searched," but rather than describe a place, the Attachment describes a process by which the place to be searched can in the future be ascertained by a Government controlled "computer server." In its entirety, Attachment A reads:

---

9 The Court acknowledges that every other court to consider the question of particularity under the facts of this case has concluded that the NIT warrant was sufficiently particular. *See United States v. Acevedo-Lemus*, No. SACR 15-137-CJC, 2016 WL 4208436, at *7 n.4 (C.D. Cal. Aug. 8. 2016) (collecting a sample of cases).

Attachment A
Place to be Searched

> This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.
>
> The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL – upf45jv3bziuctml.onion – which will be located at the government facility in the Eastern District of Virginia.
>
> The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password. The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

ECF No. 25, Ex. 1.

As there is no way to identify at the time the search warrant *was issued*, which computers, out of all the computers on planet earth might be used to log into the TARGET WEBSITE, the NIT warrant fails to particularly describe the place to be searched. The Government argues generally that the NIT warrant is sufficiently particular because it identifies the objects of the search, the activating computers that at some unknown point in the future will log into the Playpen website. However, the NIT warrant fails the particularity requirement because it does not identify which computers will be searched until the search is actually completed.

Identification of the particular place to be searched cannot depend upon facts that have not yet occurred. A warrant must particularly describe the place to be searched at the time it is issued. Just as a warrant must be supported by probable cause at the time it is issued, this Court concludes that the warrant must particularly describe the place to be searched when it is issued.

As the Grubbs Court explained regarding the probable cause for anticipatory warrants, "[a]nticipatory warrants are, therefore, no different in principle from ordinary warrants. They require the magistrate to determine (1) that it is *now probable* that (2) contraband, evidence of a crime, or a fugitive *will be* on the described premises (3) when the warrant is executed." *United States v. Grubbs*, 547 U.S. 90, 96 (2006) (emphasis added).

Agent Macfarlane's affidavit in support of the NIT warrant described the process by which the NIT malware would be deployed by a computer server operating the TARGET WEBSITE. First, a user must take the necessary steps to enter the Tor network; second, a user must ascertain the Playpen URL via a Tor network hidden service; third, a user using a computer whose location and description are entirely unknown to the issuing Magistrate Judge or the affiant must log into the TARGET WEBSITE entering a username and password; fourth, the user's entry into the website would cause their computer, located anywhere in the world, to activate the deployment of the NIT malware from the Government server in Virginia; fifth, the NIT would travel via the internet to the user's computer, implant, and search for the identifying packet of information; sixth, the NIT would harvest the identifying packet of information; seventh, the NIT would force the activating computer to send the identifying packet of information back to the Government controlled server in Virginia. Only with that information could the Government begin to describe with any particularity the computers to be searched; however, at that point, the computer had already been searched. Put differently, neither the Magistrate Judge nor the affiant could know what computers might be searched, until after the search has already occurred.

Here, describing the place to be searched as "the computer . . . of any user or administrator who logs into the TARGET WEBSITE," does not describe with particularity the

computers to be searched at the time the warrant was issued because any computer on earth could be so used. As neither the Magistrate Judge nor the affiant know which computers are to be searched until after the search has already occurred, the NIT warrant fails to particularly describe the place to be searched.

Courts will often permit the issuance of anticipatory search warrants, where the existence of probable cause is dependent upon the occurrence of some triggering, condition precedent. *Id.* at 95 (quoting W. LaFave, Search and Seizure § 3.7(c), p. 398 (4th ed. 2004)). But in cases of an anticipatory warrant, the question is simply whether there is currently probable cause to believe that evidence will be found at the particularly described location, if the anticipated event occurs. *See, e.g.*, *United States v. Tagbering*, 985 F.3d 946, 949 (8th Cir. 1993) (concluding that an affidavit, which stated that "[the affiant] anticipates that the controlled delivery of [marijuana] to 10557 Cypress, Apt. D, will occur on 8–16–91. If delivery does not occur on 8–16–91 a second delivery attempt will be made to deliver the package on 8–17–91" sufficiently stated when the condition precedent would occur); *United States v. Schwarte*, 645 F.3d 1022, 1025 (8th Cir. 2011) (concluding that an affidavit, which provided "beginning April 9, 2007, the package [of child pornography recordings] would be attempted to be delivered to the [defendant's address] . . . [i]f no one was at the [defendant's] address to accept the package, delivery would be attempted again . . . up to the 10 days allowed by the requested search warrant" sufficiently stated when the condition precedent would occur). This Court is not aware of any case where a court has permitted the actual identification of the place to be searched to depend upon the occurrence of an anticipated event that has not yet occurred.

4. Even if the NIT Warrant Was Valid, Its Scope Was Limited to Computers in the Eastern District of Virginia

a. The Search of Carlson's Computer Was Excessive in Scope

In addition to particularity, Carlson argues that the NIT warrant explicitly limited searches to property, activating computers, located in the Eastern District of Virginia. ECF No. 24 at 8; ECF No. 34 at 13. As a result, Carlson argues that the search of his activating computer in Minnesota exceeded the scope of the issued NIT warrant. *Id.* The Government contends that while only "the NIT Warrant cover sheet explicitly references the [Eastern District of Virginia], it also reference Attachments A and B, which inform the scope of the NIT Warrant." ECF No. 36 at 11. The Government further argues that the Agent Macfarlane's affidavit, which stated that the NIT malware "may cause an activating computer – wherever – located to send" identifying packets of information, should be considered in contouring the scope of the NIT warrant. *Id.*

The Court concludes that the search of Carlson's activating computer in Minnesota was improper and exceeded the scope of the NIT warrant. The language in the NIT warrant was plain and distinctive: Attachment A provided the *what*, that any activating computer that entered the Playpen website would be subject to search through the NIT deployment, but in no way altered the *where*, that searches of activating computers would take place in the Eastern District of Virginia. The Court cannot accept the Government's argument that because Attachment A does not qualify where searches will take place that NIT *warrant itself* should be read to permit the search of any activating computer. To do so, practically speaking, would be to contradictorily ignore the warrant's specific geographic limitation, that searches would be conducted in the Eastern District of Virginia, in favor of an attachment that is geographically silent. *See Fiorito*

640 F.3d at 346 (reasoning that Fourth Amendment particularity is a standard of practical accuracy).

In addition, assuming *arguendo* that Agent Macfarlane's affidavit should be considered in determining the scope of searches executed pursuant to the NIT warrant, the Court still concludes that Agents unconstitutionally expanded the scope of the NIT warrant by searching Carlson's computer located outside the Eastern District of Virginia. "[I]f officers unlawfully expanded the search beyond the scope permitted by the *warrant*" a defendant may "obtain suppression" of evidence. *United States v. Alexander*, 574 F.3d at 484, 488 (8th Cir. 2009) (emphasis added). To conclude otherwise would be to permit Agent MacFarlane's affidavit, which ambiguously states that identifying packets of information would be seized from activating computers, "wherever located," to shape the scope of the NIT warrant, when the text of the warrant itself cabined searches to the Eastern District of Virginia. The Court cannot conclude that the term "any" in Attachment A or "wherever" in Agent Macfarlane's affidavit expanded the scope of a single warrant, with identifiable and discrete territorial boundaries, to constitutionally authorize the search of any activating computer outside of that boundary, i.e., any activating computer on earth. Moreover, the Court is aware of no legal authority which stands for the proposition that an affidavit, whether incorporated or not, can expand the scope of a warrant beyond its express limitations; especially an affidavit in direct contradiction to the issued warrant.

b. Leon Good-Faith Does Not Apply

Where a warrant is sufficiently facially deficient, for example, where it "fail[s] to particularize the place to be searched or the things to be seized . . . executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923. "This exception relate[s] to alleged

infirmities with the warrant itself rather than the affidavit behind the warrant." *United States v. Carpenter*, 341 F.3d 666, 673 (8th Cir. 2003). "It is incumbent on the officer executing a search warrant to ensure the search is lawfully authorized and lawfully conducted." *Groh v. Ramirez*, 540 U.S. 551, 563, n.8 (2004).[10] "[T]he officer's reliance on the magistrate's probable-cause determination and on the technical sufficiency of the warrant he issues must be objectively reasonable . . . and it is clear that in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." *Leon*, 468 U.S. at 923. "The Fourth Amendment's particularity requirement assures the subject of the search that a magistrate has duly authorized the officer to conduct a search of limited scope. This substantive right is not protected" when an agent "fails to take the time to . . . detect a glaring defect that . . . is of constitutional magnitude." *Groh*, 540 U.S. at 565, n.9.

Here, "[t]here was no ambiguity on the face of" the NIT warrant; the warrant "specifically identified" the location of the searches of activating computers: the Eastern District of Virginia. *Carpenter*, 341 F.3d at 673. No reasonable officer could believe that the NIT warrant, which plainly limited searches to the Eastern District of Virginia, issued by the Magistrate Judge sitting in the Eastern District of Virginia, could constitutionally authorize the search of activating computers in Minnesota, or anywhere in the world. The Government argues that Agents "can hardly be faulted for failing to understand the intricacies of the jurisdiction of federal magistrate judges." ECF No. 25 at 27. However, Agents executing the NIT warrant are not being 'faulted' by this Court for failing to understand magistrate jurisdiction. Rather, the *Leon* good-faith exception does not apply on the facts of this case because the constitutional

---

10 Although *Groh* was decided in the context of qualified immunity, the Court explained that the same standard of objective reasonableness is applied in qualified immunity as in the context "of suppression in . . . *Leon*." *Groh*, 540 U.S. at 566, n.8 (quoting *Malley v. Briggs*, 475 U.S. 335, 344 (1986)).

defect in the execution of the NIT warrant was a creation of the Agents themselves, impermissibly expanding the scope and conducting searches outside the area in which the NIT warrant plainly limited searches to. That is a constitutional failure of the Agents neglecting to "tailor" their search to the NIT warrant's expressed limitations. *Garrison v. Maryland*, 480 U.S.79, 84 (1987). In addition, under the circumstances of this particular case, the NIT warrant was so facially deficient in failing to particularize what computers would be searched at the time in which the warrant was issued that the executing officer could not reasonably presume it to be valid, precluding application of the *Leon* good-faith exception. *Leon*, 468 U.S. at 923. Therefore, the evidence obtained pursuant to the NIT warrant should be suppressed.

B. Motion to Suppress Statements (ECF No. 22)

Carlson argues that his November 2, 2015, and November 17, 2016, statements constitute fruit of the defective NIT warrant, and the statements were made without the assistance of counsel in violation of the Fifth and Sixth Amendments. *See* Mot. to Supp. 2, ECF No. 22. The Government argues that Carlson was not in custody, and therefore, not entitled to *Miranda* warnings during his November 2, 2015, statement, and that he waived his Fifth and Sixth Amendment rights during his November 17, 2016, statement. ECF No. 36 at 13–23.

1. The November 2, 2015, Statement

The Fifth Amendment ensures that no person "shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. "The basic rule of *Miranda* is that an individual must be advised of the right to be free from compulsory self-incrimination, and the right to the assistance of an attorney, any time a person is taken into custody for questioning." *United States v. Griffin*, 922 F.2d 1343, 1347 (8th Cir. 1990) (citing *Miranda v. Arizona*, 384 U.S. 436, 444 (1966)). In other words, law enforcement officers must inform suspects of their

Fifth Amendment rights before subjecting them to "custodial interrogations." *Id.* The term "interrogation" under *Miranda* "refers not only to express questioning, but also to any words or actions on the part of the police (other than those normally incident to arrest and custody) that the police should know are reasonably likely to elicit an incriminating response from the suspect." *Rhode Island v. Innis*, 446 U.S. 291, 301 (1980). Additionally, "[a]n individual is in custody [for *Miranda* purposes] when placed under formal arrest, or when his or her freedom is restricted to a degree akin to formal arrest." *United States v. Elzahabi*, 557 F.3d 879, 883 (8th Cir. 2009) (citing *United States v. Ollie*, 442 F.3d 1135, 1137 (8th Cir. 2006).

It is undisputed that prior to, and during, the November 2, 2015, questioning by Agents Moule and Blackmore, Carlson was not informed of his *Miranda* rights. *See* ECF No. 36 at 14. Thus the question before this Court is whether this statement was the product of: (1) an interrogation; (2) while "in custody" for Fifth Amendment purposes. *Griffin*, 922 F.2d at 1347.

The Court concludes that Carlson was interrogated by Agents Moule and Blackmore. Agents were present at Carlson's residence pursuant to the NIT warrant for the purpose of searching a residence connected to an IP address from which child pornography was allegedly downloaded and distributed. Agents Moule and Blackmore knew of the Playpen investigation, the alleged pornographic content connected to the IP address, and their questions were calculated to gather evidence connecting Carlson to that activity. Indeed, during the February 8, 2017, hearing, Agent Moule testified that his purpose in speaking to Carlson was to gain incriminating information from him. Agents Moule and Blackmore reasonably knew their questions were likely to elicit an incriminating response from Carlson. *See Innis*, 446 U.S. at 301.

Whether Carlson was in custody during the interview turns on whether, under the totality of the circumstances, "a reasonable person in [Carlson's] position would have felt free to end the

interrogation and leave." *Elzahabi*, 557 F.3d at 883. The Eighth Circuit has invoked a nonexclusive, six-factor test to guide a court in making a custodial determination:

> (1) whether the suspect was informed at the time of questioning that the questioning was voluntary, that the suspect was free to leave or request the officers to do so, or that the suspect was not considered under arrest;
>
> (2) whether the suspect possessed unrestrained freedom of movement during questioning;
>
> (3) whether the suspect initiated contact with authorities or voluntarily acquiesced to official requests to respond to questions;
>
> (4) whether strong arm tactics or deceptive stratagems were employed during questioning;
>
> (5) whether the atmosphere of the questioning was police dominated; or
>
> (6) whether the suspect was placed under arrest at the termination of the questioning.

Griffin, 922 F.2d at 1349. However, "custody cannot be resolved merely by counting up the number of factors on each side of the balance and rendering a decision accordingly . . . the ultimate inquiry must always be whether the defendant was restrained as though he were under formal arrest." *United States v. Czichray*, 378 F.3d 822, 827–28 (8th Cir. 2004).

Based on the totality of the circumstances, the Court concludes that Carlson was not in custody during the November 2, 2015, interrogation. Testimony at the February 8, 2017, hearing, established that Agent Moule advised Carlson that he was not under arrest, the interview was voluntary, and that he could terminate the interview at any time. The recording of the interview corroborates Agent Moule's testimony; Carlson was advised that he was not under arrest, he was free to leave, he was free to terminate the interrogation, and he was free to go about his business. *See generally* Gov't. Ex. 1. Testimony further established that Carlson was not handcuffed, and his freedom of movement was not restrained. When Carlson requested that the interrogation move to a local park, Carlson's request was granted and he drove himself to the park where the

interrogation continued. Carlson was not placed under arrest at the conclusion of the interrogation. That Agents padded Carlson down before the interrogation and when the interrogation resumed at the park, likely favors a finding that the interrogating atmosphere was police dominated. However, Carlson offers no evidence to counter Agent Moule's testimony that he was not threatened, punished, intimidated, or deceptively promised anything for his participation in the interrogation. Indeed, the Court notes that after being informed that he could terminate the interrogation, Carlson stated that he would be willing to talk with Agents. *See generally id.* "This is not a case where a suspect sought to exercise his option of terminating the interview, only to meet resistance from his interrogators." *Czichray*, 378 F.3d at 829. Therefore, the Court finds no Fifth Amendment violation.

In addition, the Court finds no violation of Carlson's Sixth Amendment rights. The Sixth Amendment provides that "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to have the Assistance of Counsel for his defense." U.S. Const. amend. VI. It is well-established that "once the adversary judicial process has been initiated, the Sixth Amendment guarantees a defendant the right to have counsel present at all critical stages of the criminal proceedings." *Montejo v. Louisiana*, 556 U.S. 778, 786 (2009). A defendant's Sixth Amendment right to assistance of counsel in a criminal proceeding begins when the prosecution is commenced. *See Rothgery v. Gillespie Cnty. Tex.*, 554 U.S. 191, 199 (2008). The Supreme Court has pegged prosecutorial commencement to "the initiation of adversary judicial criminal proceedings—whether by way of formal charge, preliminary hearing, indictment, information, or arraignment." *Id.*; *see also United States v. Gouveia*, 467 U.S. 180, 188 (1984); *Kirby v. Illinois*, 406 U.S. 682, 689 (1972). "The rule is not 'mere formalism,' but a recognition of the point at which 'the government has committed itself to prosecute,' 'the adverse positions of [the] government and

defendant have solidified,' the accused 'finds himself faced with the prosecutorial forces of organized society, and immersed in the intricacies of substantive and procedural criminal law.'" *Rothgery*, 554 U.S. at 199 (quoting *Kirby*, 406 U.S. at 689).

Here, on November, 2, 2015, neither an indictment, information, or formal charge had been entered against Carlson, nor had a preliminary hearing or arraignment been held. The FBI was certainly investigating Carlson, but the Government had not committed itself to his prosecution. Consequently, Carlson's right to counsel under the Sixth Amendment had not yet attached. *Rothgery*, 554 U.S. at 199.

Concluding that November 2, 2015, statement was not violative Carlson's Fifth or Sixth Amendment rights, the question remains whether the statement must be suppressed as fruit of the NIT warrant violation. *See Wong Sun*, 371 U.S. at 488. The first question in making this determination is "whether there was a sufficient factual nexus between the constitutional violation"—the NIT warrant's defects under the Fourth Amendment—"and the challenged evidence"—Carlson's statement. *United States v. Yorgensen*, 845 F.3d 908, 913 (8th Cir. 2017); *see also United States v. Riesselman*, 646 F.3d 1072, 1079 (8th Cir. 2011). In this case, the issuance of the NIT warrant directly led to a search of Carlson's activating computer. Through that search, Agents obtained evidence of child pornography; evidence, which was used to secure the warrant to search Carlson's residence on November 2, 2015. Indeed, Agents would not have been present at Carlson's residence on November 2, 2015, but-for the issuance of the NIT warrant, and would not have obtained Carlson's statement but-for their presence at his residence. *See e.g.*, *Riesselman*, 646 F.3d at 1078 (holding that a defendant must at least making a showing that the alleged illegality was the but-for cause of obtaining the evidence). Thus, the Court

concludes that there was a sufficient factual nexus between the predicate Fourth Amendment violation and Carlson's November 2, 2015, statement.

The second question is whether the attenuation doctrine applies under *Brown v. Illinois*, 422 U.S. 590, 601 (1975), and its progeny. *See Yorgensen*, 845 F.3d at 914. The attenuation doctrine provides that, "evidence is admissible when the connection between unconstitutional police conduct and the evidence is remote or has been interrupted by some intervening circumstance." *Utah v. Strieff*, —— U.S. ——, 136 S. Ct. 2056, 2061 (2016). The attenuation doctrine examines "whether the causal connection between incriminating statements and an arrest or *search* that violated the Fourth Amendment has been broken." *Yorgensen*, 845 F.3d at 914 (emphasis added). In *Brown*, the Supreme Court elucidated the relationship between the attenuation doctrine and the Fourth and Fifth Amendments in the context of statement suppression. *See Brown*, 422 U.S. at 601. The Court explained that:

> [It has long] observed that the Fifth Amendment is in intimate relation with the Fourth, . . . [t]hus even if . . . statements . . . were found to be voluntary under the Fifth Amendment, the Fourth Amendment issue remains. In order for the causal chain, between [a Fourth Amendment violation] and the statement made subsequent thereto to be broken. *Wong Sun* requires not merely that the statement meet the Fifth Amendment standard of voluntariness, but that it be sufficiently an act of free will to purge the primary taint. . . . But the *Miranda* warnings, alone and per se, cannot always make the act sufficiently a product of free will [to] break, for Fourth Amendment purposes, the causal connection between the illegality and the confession. . . . *Miranda* warnings are an important factor, to be sure, in determining whether the confession is obtained by exploitation of a [Fourth Amendment violation]. But they are not the only factor to be considered. [In addition:] [(1) t]he temporal proximity of the arrest and the confession[;] (2) the presence of intervening circumstances[;] and, particularly, [3] the purpose and flagrancy of the official misconduct are all relevant.

Brown, 422 U.S. at 601–04 (internal citations omitted).

The Court concludes that the taint of the initial Fourth Amendment violation, the issuance of the NIT warrant, had not been purged at the time of Carlson's November 2, 2015, statement. First, the uncontroverted record shows that Carlson was not provided with a *Miranda* warning prior to the statement. *See Rawlings v. Kentucky*, 448 U.S. 98, 110 (1980). Second, Carlson's interrogation began immediately after the execution of the warrant. *But cf. United States v. Whisenton*, 765 F.3d 938, 941–42 (8th Cir. 2014); *United States v. Barnum*, 564 F.3d 964, 972 (8th Cir. 2009) (holding that fifteen minutes was sufficient to demonstrate an attenuation of illegality). Third, there were no intervening circumstances to purge the taint of the defective warrant. Specifically, there were no intervening circumstances between the NIT warrant and the execution of the search warrant of Carlson's residence to break the causal chain. Fourth, the purpose and flagrancy of the FBI's misconduct in attempting to obtain the NIT warrant and deploying the NIT malware is truly staggering. In order to identify Playpen users, the FBI operated a copied version of a dark web, child pornography website for two weeks. During that period, countless images and video content depicting child pornography were globally downloaded and distributed via the Playpen. In essence, the FBI facilitated the victimization of minor children and furthered the commission of a more serious crime—the distribution of child pornography—to primarily identify offenders committing less serious crimes—viewing and receipt of child pornography. Moreover, although the January 15, 2015, warrant obtained by Agent Alfin judicially authorized the FBI to seize the Playpen's domain URL, that warrant did not authorize the FBI to then independently operate the website and house and disseminate the very content it now accuses hundreds of defendants of receiving. Therefore, the Court concludes that Carlson's November 2, 2015, statement was not purged of the taint of the NIT warrant's

Fourth Amendment violations and suppression of that statement is justified on the facts of this case. *See Brown*, 422 U.S. at 601–04.

2. The November 17, 2016, Statement

Carlson argues his November 17, 2016, statement was also the fruit of the Fourth Amendment violation and was given in violation of his Fifth and Sixth Amendment rights. ECF No. 22 at 2. The Government argues that Carlson waived his Fifth and Sixth Amendment rights. ECF No. 36 at 20–23.

As a threshold matter, Carlson's November 17, 2016, statement was given after he was placed in custody on the arrest warrant issued the previous day. In order for evidence obtained as a result of a custodial interrogation to be used against a defendant at trial, the Fifth Amendment requires that law enforcement advise the defendant of his constitutional rights and that the defendant make a valid waiver of those rights. *See Miranda*, 384 U.S. at 444. Before questioning begins, a suspect in custody must be informed of the following: (1) that he has the right to remain silent; (2) that his statements may be used against him in a court of law; (3) that he has the right to an attorney; and (4) that if he cannot afford an attorney, one will be appointed. *Id.* at 444, 469–70, 478–79. After the warnings are given, if the suspect indicates that he wishes to assert these rights, the interrogation must stop. *See id.* at 473–74. Statements elicited from a suspect in violation of *Miranda* are inadmissible. *See Stansbury v. California*, 511 U.S. 318, 322 (1994).

Once advised of *Miranda* rights, a suspect's waiver of his Fifth Amendment privilege against self-incrimination is only valid if it is voluntarily, knowingly, and intelligently made. *See Miranda*, 384 U.S. at 444; *Berghuis v. Thompkins*, 560 U.S. 370, 382 (2010); *United States v. Syslo*, 303 F.3d 860, 866 (8th Cir. 2002). A waiver is made knowingly if it is "made with a full

awareness of both the nature of the right abandoned and the consequences of the decision to abandon it." *Moran v. Burbine*, 475 U.S. 412, 421 (1986). It is voluntary if it is "the product of a free and deliberate choice rather than intimidation, coercion, or deception." *Id.* It is the Government's burden to show that the suspect's waiver meets these standards. *Miranda*, 384 U.S. at 475.

A defendant's Sixth Amendment right is violated whenever, in the absence of counsel, federal Agents deliberately elicit statements from him. *See Massiah v. United States*, 377 U.S. 201, 204–205 (1964). The Supreme Court has consistently applied the "deliberate elicitation" standard to Sixth Amendment violations, and expressly distinguished it from the custodial interrogation standard applicable to Fifth Amendment violations. *See United States v. Fellers*, 540 U.S. 519, 524 (2004). While courts continue to apply different standards to the Fifth and Sixth Amendments to determine whether a violation has occurred, the standard for whether there has been a waiver of rights is the same under both the Fifth and Sixth Amendments; whether the waiver was voluntary, knowing, and intelligent. *See Montejo*, 556 U.S. at 786–87.

A defendant may waive his Sixth Amendment right "whether or not he is already represented by counsel; the decision to waive need not itself be counseled." *Id.* at 786. "And when a defendant is read his *Miranda* rights (which include the right to have counsel present during interrogation) and agrees to waive those rights, that typically does the trick, even though the *Miranda* rights purportedly have their source in the *Fifth* Amendment." *Id.* (emphasis in original) (citing *Patterson v. Illinois*, 487 U.S. 285, 296 (1988) ("As a general matter . . . an accused who is admonished with the warnings prescribed by this Court in *Miranda* . . . has been sufficiently apprised of the nature of his Sixth Amendment rights, and of the consequences of

abandoning those rights, so that his waiver on this basis will be considered a knowing and intelligent one.")).

The Court concludes that Carlson knowingly, voluntarily, and intelligently waived his Fifth and Sixth Amendment rights prior to his November 17, 2016, statement. Shortly after his arrest, but before the interrogation began, Carlson read and signed an Oral Warnings to be Given to a Suspect Prior to Interrogation Form, apprising him of his: right to remain silent; that statements may be used against him; right to counsel; and right to have an attorney provided. *See* Gov't. Ex. 3. Testimony at the February 8, 2017, hearing established that Carlson did not appear to be under the influence of drugs or alcohol, appeared to be oriented to time and place, and appeared to fully understand Agent Moule's questions.

After signing the form, Carlson stated that after the November 2, 2015, interview, he sought the advice of an attorney and was advised that he should not speak with Agents regarding the investigation. *See* Gov't. Ex. 2 at 1:13–1:17. The attorney also advised Carlson that speaking with law enforcement and making inadvertent inculpatory statements exposed him to potential criminal liability. *Id.* However, Carlson also stated that not talking with Agents "sucks because I am not that type of person . . . and I want things to be right, and I'm incriminating myself by saying anything, . . . [but] do I believe I need help, I do . . . you know, I want things to be right, and to live this life is crazy." *Id.* Later in the interview, Carlson identified a series of images allegedly depicting child pornography and stated that the images were captured in his former residence on an old camera that has since been stolen. *Id.* at 1:30–1:36.

The uncontroverted record shows that Carlson was aware of his right to counsel and his right against self-incrimination. Nonetheless, Carlson proceeded with the interrogation on his own volition because he wanted "things to be right." *Id.* Under the totality of the circumstances,

the record supports a finding that Carlson abandoned his Fifth and Sixth Amendment rights. *See Patterson*, 487 U.S. at 296.

Concluding that the November 17, 2016, statement was not violative of the Fifth or Sixth Amendment, the question remains whether it must be suppressed as fruit of the Fourth Amendment violation. Specifically, whether there was a factual nexus between the Fourth Amendment violation and whether the taint of the violation had been attenuated applying the *Brown* factors. The Court concludes that there was a factual nexus between the constitutional violation—the NIT warrant's defects under the Fourth Amendment—and the challenged evidence—Carlson's statement. *See supra* at 34.

As to the *Brown* attenuation factors, first, although apprising a suspect of their *Miranda* rights is not controlling, that Carlson was given his *Miranda* warning is an *important* factor in the *Brown* analysis. *Brown*, 422 U.S. at 601 (emphasis added). Second, the Court observes the presence of several intervening factors. The NIT warrant had been issued over twenty months before his arrest, and Carlson's first NIT related interrogation had taken place over a year before. In the intervening period, Carlson had contacted an attorney, was advised not to speak with law enforcement, and was counseled on the potential incriminating consequences of doing so. *See* Gov't. Ex. 2 at 1:13. By November 17, 2016, Carlson was very much aware of the nature and purpose of the investigation, knew he was a suspect in that investigation, and had ample "opportunit[y] to pause and reflect, and to decline consent after deliberate consideration if [he] wished." *United States v. Brandwein*, 796 F.3d 980, 986 (8th Cir. 2015). Accordingly, Carlson's November 17, 2016, statement was sufficiently a product of free will to purge the taint of the NIT warrant's manifold constitutional defects and the purpose and flagrancy of the misconduct

exhibited during the execution of the NIT warrant. Therefore, this statement must not be suppressed.

III. RECOMMENDATION

Based upon the foregoing, and all of the files, records, and proceedings herein, **IT IS HEREBY RECOMMENDED** that:

1. Carlson's motion to suppress statements (ECF No. 22) be **GRANTED in part** and **DENIED in part** as follows:

   a. Carlson's request to suppress his November 2, 2015, statement be **GRANTED;**

   b. Carlson's request to suppress his November 17, 2016, statement be **DENIED**.

2. Carlson's motion to suppress evidence obtained as a result of search and seizure (ECF No. 23) be **GRANTED**.

DATED: March 23, 2017

s/Franklin L. Noel

FRANKLIN L. NOEL
United States Magistrate Judge

Pursuant to the Local Rules, any party may object to this Report and Recommendation by filing with the Clerk of Court and serving on all parties, on or before **April 6, 2017**, written objections that specifically identify the portions of the proposed findings or recommendations to which objection is being made, and a brief in support thereof. A party may respond to the objecting party's brief within fourteen (14) days after service thereof. All briefs filed under the rules shall be limited to 3,500 words. A judge shall make a de novo determination of those portions to which objection is made.

Unless the parties are prepared to stipulate that the District Court is not required by 28 U.S.C. § 636 to review a transcript of the hearing in order to resolve all objections made to this Report and Recommendation, the party making the objections shall timely order and cause to be filed by **April 6, 2017** a complete transcript of the hearing.

This Report and Recommendation does not constitute an order or judgment of the District Court, and it is, therefore, not appealable to the Circuit Court of Appeals.